AMENDMENT TO THE CLAIMS

1   1.   (Currently amended) A method for sharing a secure

2   communication session with a client between a plurality of servers, comprising:

3   receiving a message from the client at a first server in the plurality of

4   servers, the message including a session identifier that identifies a secure

5   communication session with the client; and

6   if the session identifier does not correspond to an active secure

7   communication session on the first server, establishing an active secure

8   communication session with the client on the first server by,

9   attempting to retrieve state information associated with the

10   session identifier for an active secure communication session

11   between the client and a second server from the plurality of

12   servers,

13   if the state information for the active secure communication

14   session is retrieved, using the state information to establish the

15   active secure communication session with the client without

16   having to communicate with the client, whereby the secure

17   communication session is transferred from the client and the

18   second server to the client and the first server without incurring the

19   overhead of establishing a new secure connection, and

20   if the state information for the active secure communication

21   session is not retrieved, communicating with the client to establish

22   the active secure communication session with the client.

1   2.   (Original) The method of claim 1, wherein attempting to retrieve

2   the state information includes:

3   attempting to use the session identifier to identify the second server in the

4 plurality of servers that has an active secure communication session with the

5 client that corresponds to the session identifier; and

6   attempting to retrieve the state information from the second server.

1   3.   (Original) The method of claim 1, wherein attempting to retrieve

2 the state information involves attempting to retrieve the state information from a

3 centralized repository that is in communication with the plurality of servers.

1   4.   (Original) The method of claim 3, wherein the centralized

2 repository includes a database for storing the state information.

1   5.   (Original) The method of claim 1, wherein establishing the active

2 secure communication session involves establishing a secure sockets layer (SSL)

3 connection with the client.

1   6.   (Original) The method of claim 1, wherein the state information

2 includes:

3   a session encryption key for the secure communication session;

4   the session identifier for the secure communication session; and

5   a running message digest for the secure communication session.

1   7.   (Original) The method of claim 6, further comprising:

2   using the message to update the running message digest; and

3   checkpointing the updated running message digest to a location outside of

4 the first server.

4

8.   (Original) The method of claim 1, further comprising, if the state information for the active secure communication session is retrieved, purging the state information from a location from which the state information was retrieved, so that the state information cannot be subsequently retrieved by another server in the plurality of servers.

9.   (Original) The method of claim 1, further comprising initially establishing an active secure communication session between the client and the second server, the active secure communication session being identified by the session identifier.

10.   (Original) The method of claim 1, wherein attempting to retrieve the state information includes authenticating and authorizing the first server.

11.   (Cancelled)

12.   (Cancelled)

13.   (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for sharing a secure communication session with a client between a plurality of servers, the method comprising:

    receiving a message from the client at a first server in the plurality of servers, the message including a session identifier that identifies a secure communication session with the client; and

    if the session identifier does not correspond to an active secure communication session on the first server, establishing an active secure communication session with the client on the first server by,

11   attempting to retrieve state information associated with the

12   session identifier for an active secure communication session

13   between the client and a second server from the plurality of

14   servers,

15   if the state information for the active secure communication

16   session is retrieved, using the state information to establish the

17   active secure communication session with the client without

18   having to communicate with the client, whereby the secure

19   communication session is transferred from the client and the

20   second server to the client and the first server without incurring the

21   overhead of establishing a new secure connection, and

22   if the state information for the active secure communication

23   session is not retrieved, communicating with the client to establish

24   the active secure communication session with the client.

1   14.   (Original) The computer-readable storage medium of claim 13,

2   wherein attempting to retrieve the state information includes:

3   attempting to use the session identifier to identify the second server in the

4   plurality of servers that has an active secure communication session with the

5   client that corresponds to the session identifier; and

6   attempting to retrieve the state information from the second server.

1   15.   (Original) The computer-readable storage medium of claim 13,

2   wherein attempting to retrieve the state information involves attempting to

3   retrieve the state information from a centralized repository that is in

4   communication with the plurality of servers.

16. (Original) The computer-readable storage medium of claim 15, wherein the centralized repository includes a database for storing the state information.

17. (Original) The computer-readable storage medium of claim 13, wherein establishing the active secure communication session involves establishing a secure sockets layer (SSL) connection with the client.

18. (Original) The computer-readable storage medium of claim 13, wherein the state information includes:
   a session encryption key for the secure communication session;
   the session identifier for the secure communication session; and
   a running message digest for the secure communication session.

19. (Original) The computer-readable storage medium of claim 18, wherein the method further comprises:
   using the message to update the running message digest; and
   checkpointing the updated running message digest to a location outside of the first server.

20. (Original) The computer-readable storage medium of claim 13, wherein the method further comprises, if the state information for the active secure communication session is retrieved, purging the state information from a location from which the state information was retrieved, so that the state information cannot be subsequently retrieved by another server in the plurality of servers.

21.   (Original) The computer-readable storage medium of claim 13, wherein the method further comprises initially establishing an active secure communication session between the client and the second server, the active secure communication session being identified by the session identifier.

22.   (Original) The computer-readable storage medium of claim 13, wherein attempting to retrieve the state information includes authenticating and authorizing the first server.

23.   (Cancelled)

24.   (Cancelled)

25.   (Currently amended) An apparatus that shares a secure communication session with a client between a plurality of servers, comprising:

a receiving mechanism, at a first server in the plurality of servers, that receives a message from the client, the message including a session identifier that identifies a secure communication session with the client;

an examination mechanism that examines the session identifier; and

a session initialization mechanism, on the first server, wherein if the session identifier does not correspond to an active secure communication session on the first server, the session initialization mechanism is configured to establish an active secure communication session with the client by,

attempting to retrieve state information associated with the session identifier for an active secure communication session between the client and a second server from the plurality of servers,

8

Sub B²₁₅

16 if the state information for the active secure communication

17 session is retrieved, using the state information to establish the

18 active secure communication session with the client without

19 having to communicate with the client, whereby the secure

20 communication session is transferred from the client and the

21 second server to the client and the first server without incurring the

22 overhead of establishing a new secure connection, and

23 if the state information for the active secure communication

24 session is not retrieved, communicating with the client to establish

   the active secure communication session with the client.

1 26. (Original) The apparatus of claim 25, wherein the session

2 initialization mechanism is configured to attempt to retrieve the state information

3 by:

4 attempting to use the session identifier to identify the second server in the

5 plurality of servers that has an active secure communication session with the

6 client that corresponds to the session identifier; and

7 attempting to retrieve the state information from the second server.

1 27. (Original) The apparatus of claim 25, wherein the session

2 initialization mechanism is configured to attempt to retrieve the state information

3 by attempting to retrieve the state information from a centralized repository that is

4 in communication with the plurality of servers.

1 28. (Original) The apparatus of claim 27, wherein the centralized

2 repository includes a database for storing the state information.

29.   (Original) The apparatus of claim 25, wherein the active secure
communication session includes a secure sockets layer (SSL) connection with the
client.

30.   (Original) The apparatus of claim 25, wherein the state information
includes:
        a session encryption key for the secure communication session;
        the session identifier for the secure communication session; and
        a running message digest for the secure communication session.

31.   (Original) The apparatus of claim 30, further comprising an
updating mechanism that is configured to:
        use the message to update the running message digest; and to
        checkpoint the updated running message digest to a location outside of the
first server.

32.   (Original) The apparatus of claim 25, further comprising a purging
mechanism that is configured to purge the state information from a location from
which the state information was retrieved, so that the state information cannot be
subsequently retrieved by another server in the plurality of servers.

33.   (Original) The apparatus of claim 25, wherein the session
initialization mechanism is configured to authenticate and authorize the first
server prior to receiving the state information.

34.   (Cancelled)

35.   (Cancelled)

10